CLAIMS

1. A secured communication method for a mobile communications network, the method comprising:

receiving a request to provide a security key to a mobile device connected to the mobile communications network;

generating a unique security key for the requesting mobile device;

forwarding the unique security key to the mobile device;

receiving a request to provide the unique security key for the mobile device to a service provider; and

providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device.

2. The method of claim 1, further comprising:

denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device.

3. The method of claim 1, further comprising:

storing the unique security key in the mobile device's data storage mechanism.

4. The method of claim 3, wherein the data storage mechanism is a memory chip.

5. The method of claim 3, wherein the data storage mechanism is an identity module for the mobile device.

6. The method of claim 3, wherein the data storage mechanism is a SIM card for the mobile device.

7. The method of claim 1, further comprising:

storing the unique security key in a data structure in association with a unique value identifying the mobile device.

8. The method of claim 7, wherein the unique value is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) and phone number.

9. The method of claim 1, further comprising:

determining if the service provider is approved based on content of a list of approved service providers.

10. The method of claim 9, wherein the list of approved service providers is stored in the mobile device.

11. A security system for managing security key assignment in a mobile communications terminal, the security system comprising:

a key generating mechanism for generating a unique security key for a mobile device, in response to a request received by the security system from the mobile device;

a transmission mechanism for transmitting the unique security key to the mobile device; and

a data storage mechanism for storing the unique security key for the mobile device in association with an identifier identifying the mobile device,

wherein the unique security key is transmitted to a service provider, in response to a request submitted by the service provider to the security system.

12. The security system of claim 11, further comprising:

a verification mechanism for verifying whether the service provider is an approved service provider before the unique security key is transmitted to the service provider.

13. The security system of claim 12, wherein the service provider is determined to be the approved service provider, if a first condition is met.

14. The security system of claim 13, wherein the first condition is set by the mobile device.

15. The security system of claim 14, wherein the first condition is communicated to the security system by the mobile device.